FEATURE BENEFIT SHEET

GenAI Risk Module

Ensure Safe and Controlled Use of Generative AI While Preventing Data Risks and Compliance Violations in Your Organization

The Challenge

As generative AI adoption accelerates, organizations face significant challenges in ensuring its safe and compliant use. According to Gartner, by 2026, over 80% of enterprises will have adopted generative AI, but only 40% will have security and governance measures in place. Without proper oversight, employees may inadvertently expose sensitive data, intellectual property, and personally identifiable information (PII) when interacting with AI-powered chat tools. This creates compliance risks and opens the door to data exfiltration, security breaches, and regulatory violations.

Additionally, shadow AI usage—where employees access unapproved AI applications—poses an escalating risk. Organizations must gain visibility and control over AI interactions to mitigate risks while allowing employees to harness AI's benefits in a secure and responsible manner.

The Solution

The iboss **GenAI Risk Module** solution provides comprehensive visibility, control, and risk mitigation for AI usage within organizations. As a capability of the iboss Zero Trust SASE platform, it enables businesses to log, monitor, and enforce AI policies, ensuring that AI interactions align with security and compliance requirements. The solution logs all ChatGPT conversations, allowing security teams to analyze AI usage trends while proactively detecting and preventing sensitive data exposure and policy violations.

With real-time question monitoring and automated blocking of risky queries, iboss helps prevent the accidental leakage of confidential data. The iboss GenAI Risk Module solution empowers organizations to safeguard AI interactions, reduce compliance risks, and maintain operational integrity without stifling innovation.

65%

65% of enterprises now regularly use generative AI—nearly double the adoption rate from ten months ago.

9%

Only **9%** of companies feel ready to manage Gen-AI risks, despite 93% recognizing the threats.

$5M

The average cost of a public cloud data breach, highlighting the risks of unsecured AI traffic.

Why iboss?

Comprehensive AI Security Controls

Gain full visibility into generative AI interactions while preventing data exposure, compliance violations, and unauthorized tool usage.

Seamless Protection Across Devices

Enforce AI security policies consistently across all user devices—desktops, laptops, tablets, and mobile—without disruptions.

Real-Time AI Risk Prevention

Automatically detect and block sensitive data sharing in AI prompts, safeguarding confidential information before exposure occurs.

Fully Unified + Fully Distributed

Unified Controls:

Monitor and enforce AI security policies across all users and devices, ensuring consistent oversight and risk mitigation.

Unified Protection:

Analyze AI prompts in real time to detect sensitive data, enforce compliance, and prevent unauthorized AI tool usage.

Unified Visibility:

Provide detailed logs of AI interactions, offering security teams insight into usage patterns, risks, and policy enforcement actions.

FEATURE BENEFIT SHEET

GenAI Risk Module

Ensure Safe and Controlled Use of Generative AI While Preventing Data Risks and Compliance Violations in Your Organization

Feature Capability	Feature Benefit
Chat Log Monitoring Captures and logs ChatGPT interactions, including questions and responses, to provide full visibility into AI usage within the organization.	**Full AI Usage Visibility** Enable security teams to monitor AI activity, detect anomalies, and identify trends in how employees use generative AI.
Top User and Topic Insights Provides a detailed view of top ChatGPT users, including conversation topics, to help organizations understand AI adoption and potential risks.	**Enhanced AI Governance** Help security teams enforce AI usage policies by identifying frequent users and high-risk AI interactions.
Real-Time Question Monitoring Scan AI interactions in real time to identify and block queries that contain sensitive PII, compliance violations, or confidential data.	**Proactive Risk Prevention** Prevent accidental or intentional data leaks by stopping risky AI queries before they are processed.
AI Access Controls Redirect users attempting to access unapproved generative AI tools to an approved AI platform where security policies are enforced.	**Enforce AI Policy Compliance** Ensure employees use only authorized AI tools, reducing the risk of data exposure and security breaches.
End-User Awareness Alerts Notify users that AI interactions are being monitored, promoting responsible AI usage and reinforcing security best practices.	**User Accountability** Reduce risky behavior by increasing awareness that AI conversations are subject to security oversight.
Seamless Multi-Device Support Applies AI monitoring and security policies across all device types, including desktops, laptops, tablets, and mobile devices.	**Consistent Security Across Devices** Ensure AI governance remains intact regardless of where employees access AI tools.
Real-Time AI Risk Alerting Instantly notify security teams when high-risk AI activity, such as unauthorized data sharing or policy violations, is detected.	**Faster Incident Response** Enable immediate action on potential security threats, reducing exposure time and mitigating risks before escalation.
Transparent Logging & Reporting Generates detailed AI activity reports with searchable logs for compliance audits, security investigations, and policy enforcement.	**Regulatory Compliance Support** Meet data security and compliance requirements by providing auditable AI interaction records.

Conclusions

Relying on AI Platform Security is Not Enough
Built-in AI safeguards lack full visibility and control, leaving organizations vulnerable to data leaks and compliance violations.

Consistent AI Security Across All Users and Devices
A solution that is both Fully Unified and Fully Distributed ensures seamless enforcement of AI policies regardless of location or device.

Real-Time AI Risk Prevention is Essential
Blocking sensitive queries and unauthorized AI access in real time reduces security incidents and strengthens enterprise data protection.

More Information

Contact Us

The iboss Zero Trust SASE platform delivers comprehensive security and compliance from a single, centralized console. With built-in encryption, seamless policy enforcement, and full visibility across your Users & Applications real-estate, the platform simplifies management while protecting sensitive data across all devices and locations.

Request a Demo Today